JP7036672

Publication Title:

RANDOM-NUMBER GENERATOR, COMMUNICATION SYSTEM USING THE SAME AND METHOD THEREFOR

Abstract:

PURPOSE:To generate a safe random number sequence at a high speed.

CONSTITUTION:This generator is provided with a shift register 1 bonding data, a linear conversion circuit 12 inputting the data held in the shift register 11 and converting an inputted data value based on a prescribed parameter, an update means updating the data held in the shift register 11 based on the conversion result by the linear conversion circuit 12 and an output means successively outputting the partial data held in the shift register 11 as a random number sequence.

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－36672

(43)公開日　平成７年(1995)２月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58	Ｃ			
Ｇ０９Ｃ　1/00		8837－5Ｌ		
Ｈ０４Ｌ　9/22				
			Ｈ０４Ｌ　9/ 04	

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願平5－179232

(22)出願日　平成５年(1993)７月20日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　山本　貴久
東京都大田区下丸子３丁目30番２号キヤノン株式会社内

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号キヤノン株式会社内

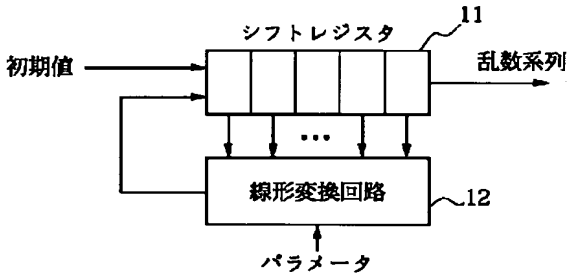
(74)代理人　弁理士　丸島　儀一

(54)【発明の名称】　乱数発生器、及びそれを用いた通信システム及びその方法

(57)【要約】

【目的】　高速かつ安全な乱数系列を発生する。

【構成】　データを保持するシフトレジスタ１１と、該シフトレジスタ１１に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する線形変換回路１２と、該線形変換回路１２による変換結果に基づき、前記シフトレジスタ１１に保持されるデータを更新する更新手段と、前記シフトレジスタ１１に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。



1

【特許請求の範囲】

【請求項１】　データを保持する保持手段と、
該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、
該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、
前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具え、前記パラメータを所定の周期で変更することを特徴とする乱数発生器。

【請求項２】　データを保持する保持手段と、
該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、
該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、
前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する算出手段とを具えることを特徴とする乱数発生器。

【請求項３】　データを保持する第１の保持手段と、
該第１の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第１の変換手段と、
該第１の変換手段による変換結果に基づき、前記第１の保持手段に保持されるデータを更新する第１の更新手段と、
前記第１の保持手段に保持されるデータの一部を、乱数系列として順次出力する第１の出力手段と、
該第１の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、
データを保持する第２の保持手段と、
該第２の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第２の変換手段と、
該第２の変換手段による変換結果に基づき、前記第２の保持手段に保持されるデータを更新する第２の更新手段と、
前記第２の保持手段に保持されるデータの一部を、乱数系列として順次出力する第２の出力手段と、
該第２の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項４】　データを保持する第１の保持手段と、
該第１の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第１の変換手段と、
該第１の変換手段による変換結果に基づき、前記第１の保持手段に保持されるデータを更新する第１の更新手段と、

2

前記第１の保持手段に保持されるデータの一部を、乱数系列として順次出力する第１の出力手段と、
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第１の算出手段と、
前記第１の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に備え、
データを保持する第２の保持手段と、
該第２の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第２の変換手段と、
該第２の変換手段による変換結果に基づき、前記第２の保持手段に保持されるデータを更新する第２の更新手段と、
前記第２の保持手段に保持されるデータの一部を、乱数系列として順次出力する第２の出力手段と、
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第２の算出手段と、
前記第２の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具えたことを特徴とする通信システム。

【請求項５】　送信側で、データを保持する第１の保持部に保持されたデータを第１の変換部に入力し、
所定のパラメータに基づいて入力データを変換し、
該変換の結果に基づき、前記第１の保持部に保持されるデータを更新し、
前記第１の保持部に保持されるデータの一部を、乱数系列として順次出力し、
該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、
受信側で、データを保持する第２の保持部に保持されたデータを第２の変換部に入力し、
所定のパラメータに基づいて入力データを変換し、
該変換の結果に基づき、前記第２の保持部に保持されるデータを更新し、
前記第２の保持部に保持されるデータの一部を、乱数系列として順次出力し、
該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【請求項６】　送信側で、データを保持する第１の保持部に保持されたデータを第１の変換部に入力し、
所定のパラメータに基づいて入力データを変換し、
該変換の結果に基づき、前記第１の保持部に保持されるデータを更新し、
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更し、
前記第１の保持部に保持されるデータの一部を、乱数系列として順次出力し、

3

該出力される乱数系列に基づいて通信文を暗号化する暗号文を順時受信側に送信し、
受信側で、データを保持する第２の保持部に保持されたデータを第２の変換部に入力し、
所定のパラメータに基づいて入力データを変換し、
該変換の結果に基づき、前記第２の保持部に保持されるデータを更新し、
前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを更新し、
前記第２の保持部に保持されるデータの一部を、乱数系列として順次出力し、
該出力される乱数系列に基づいて暗号文を復号することを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は暗号化方式に関係し、特に暗号通信分野におけるデータの秘匿、発信者・着信者の認証、暗号鍵の共有、零知識証明プロトコル等に関するものである。また、モンテカルロシミュレーションなどの乱数を用いたシミュレーションに関するものである。

【０００２】

【従来の技術】従来、乱数発生法の一つとして、文献「現代暗号理論」（池野、小山著、昭和６１年発行、電子情報通信学会）の第６９～７２頁に示されているように、最大長周期系列（M系列）を発生する線形フィードバックシフトレジスタ（ＬＦＳＲ）を用いたものが知られている。

【０００３】ＬＦＳＲ方式とは、図１４に示すようにｓ段のシフトレジスタＲ（ｔ）＝（r_s（ｔ）、r_{s-1}（ｔ）、…、r_2（ｔ）、r_1（ｔ））とタップ（引込線）列（h_s、h_{s-1}、…、h_2、h_1）からなり、各時点（ストップ）ごとに次のような動作を同時に行うことにより、擬似乱数系列を生成する方法である。

【０００４】（ａ）最右端のレジスタのビットr_1（ｔ）を擬似乱数系列として出力する。

【０００５】k_t＝r_1（ｔ）

（ｂ）r_s（ｔ）、r_{s-1}（ｔ）、…、r_2（ｔ）を右にシフトする。

【０００６】r_i（ｔ＋１）＝r_{i+1}（ｔ）（ｉ＝１、２、…、ｓ－１）

（ｃ）最左端のレジスタのビットr_s（ｔ＋１）をレジスタの内容とタップ列により、次のように計算する。

【０００７】

【外１】

$$r_s(t+1)=\sum_{i=1}^{s} h_i \cdot r_i(t) \bmod 2$$

以上まとめると、ＬＦＳＲ方式の擬似乱数発生アルゴリズムはｓ行ｓ列の行列Ｈを用いて、

4

$$R(t+1)=H\cdot R(t) \bmod 2 \quad (1)$$

つまり、

【０００８】

【外２】

$$\begin{bmatrix} r_s(t+1) \\ r_{s-1}(t+1) \\ r_{s-2}(t+1) \\ \vdots \\ r_2(t+1) \\ r_1(t+1) \end{bmatrix} = \begin{bmatrix} h_s & h_{s-1} & \cdots & h_3 & h_2 & h_1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} r_s(t) \\ r_{s-1}(t) \\ r_{s-2}(t) \\ \vdots \\ r_2(t) \\ r_1(t) \end{bmatrix}$$

と表せる。

【０００９】このｓ段のＬＦＳＲのタップ列をうまく選ぶと、最大周期2^s-1の擬似乱数のビット系列を生成することができ、その時の系列が前述の最大長周期系列となる。

【００１０】しかしながら、このＬＦＳＲを用いる乱数発生法では、ＬＦＳＲの線形性を利用して２ｓビットの出力擬似乱数列からｓ段のタップ列（h_s、h_{s-1}、…、h_2、h_1）を以下の方法で決定できる。

【００１１】出力される擬似乱数系列がk_1、k_2、…、k_{2s}であったとすると、ある時点ｔ（ｔ＝１、２、…、ｓ＋１）のレジスタの内容Ｒ（ｔ）は、

$R(1)=(k_s, K_{s-1}, \ldots, k_1)^T$

$R(2)=(k_{s+1}, K_s, \ldots, k_2)^T$

…

$R(s+1)=(k_{2s}, K_{2s-1}, \ldots, k_{s+1})^T$

と表せる（^{T}は転置を示す）。この時、行列Ｘ、Ｙを

Ｘ＝（Ｒ（１）、Ｒ（２）、…、Ｒ（ｓ））

Ｙ＝（Ｒ（２）、Ｒ（３）、…、Ｒ（ｓ＋１））

とすると、式（１）より

Ｙ＝Ｈ・Ｘ

の関係が成立するため、

$H=Y\cdot X^{-1}$　（２）

によりＨが求められ、タップ列が決定される。

【００１２】つまり、乱数の周期は2^s-1であるがそのうち２ｓビットでＬＦＳＲの構成が決定される。この場合、その時点以降に発生される乱数列が全てわかってしまうため、出力乱数列を暗号用の乱数として用いるには安全性の面で不適当であるという欠点があった。

【００１３】また、非線形フィードバックシフトレジスタを用いれば、出力乱数系列の解析に必要となる乱数の数を大きくすることができることが知られている。しかし、バーレカンプ－マッセイのアルゴリズム（Ｅ．Ｒ．Ｂｅｒｌｅｋａｍｐ“Ａｌｇｅｂｒａｉｃ ｃｏｄｉｎｇ ｔｈｅｏｒｙ”、ＭｃＧｒａｗ－Ｈｉｌｌ Ｂｏｏｋ Ｃｏｍｐａｎｙ、１９６８）によりその系列を生成することができる最小段数のＬＦＳＲを求めることがで

き、非線形フィードバックシフトレジスタを用いた乱数発生方式も、式（２）の方法により解析される可能性があった。

【００１４】以上の様に、ある時点までの出力乱数を手に入れることができれば、それ以降に出力する乱数列全てを容易に予測することができる乱数発生方式を便宜上方式Ａと呼ぶことにする。方式Ａは上述のように暗号学的に安全ではないが、構成が容易なので高速処理が可能であるという特徴を持つ。

【００１５】方式Ａとは異なり、ある時点までに発生さ＊れた乱数列のみからその時点以降に発生されるべき乱数を予測することが非常に困難となる乱数発生法を以下に示し、便宜上方式Ｂと呼ぶことにする。

$$x_{i+1} = x_i^2 \bmod n \quad (i=0, 1, 2, \ldots) \quad (3)$$

$b_i = \mathrm{lsb}(x_i)$ $(i=0, 1, 2, \ldots)$

によって与えられる（ただし、ｎ＝ｐ・ｑ、ｌｓｂは最下位ビットを表わす）。

【００１７】この方法により生成された乱数列b_1、b_2、…、b_iのみからb_{i+1}を求めることは、ｎを因数分解するのと同じだけの手間が必要であることが知られている。つまり、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を求めるための計算量は、ｎを因数分解するのに必要な計算量と同等であることが知られている。ただし、ｎを因数分解することを計算量的に困難にするためにはｐ、ｑを数百ビット程度にする必要がある。このように、ある時点までに発生された乱数列のみからその時点以降に発生されるべき乱数を予測することが計算量的に困難となるような方法により生成された乱数は、暗号学的に安全な擬似乱数と呼ばれている。

【００１８】しかし、乱数発生法として暗号学的に安全な擬似乱数発生方式を用いた場合には、前述のようにｐ、ｑを数百ビット程度にする必要があり、その場合、式（３）の$x_{i+1} = x_i^2 \bmod n$を計算するための計算量が大きく、高速に乱数を発生できないという問題があった。

【００１９】

【課題を解決するための手段】上記課題を解決するために、本発明の乱数発生器は、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段とを具える。

【００２０】また、本発明の他の態様によれば、データを保持する保持手段と、該保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する変換手段と、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新する更新手段と、前記保持手段に保持されるデータの一部を、乱数系列として順次出力する出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する算出手段とを具える。

【００２１】また、本発明の他の態様によれば、データを保持する第１の保持手段と、該第１の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第１の変換手段と、該第１の変換手段による変換結果に基づき、前記第１の保持手段に保持されるデータを更新する第１の更新手段と、前記第１の保持手段に保持されるデータの一部を、乱数系列として順次出力する第１の出力手段と、該第１の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第２の保持手段と、該第２の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第２の変換手段と、該第２の変換手段による変換結果に基づき、前記第２の保持手段に保持されるデータを更新する第２の更新手段と、前記第２の保持手段に保持されるデータの一部を、乱数系列として順次出力する第２の出力手段と、該第２の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【００２２】また、本発明の他の態様によれば、データを保持する第１の保持手段と、該第１の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第１の変換手段と、該第１の変換手段による変換結果に基づき、前記第１の保持手段に保持されるデータを更新する第１の更新手段と、前記第１の保持手段に保持されるデータの一部を、乱数系列として順次出力する第１の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第１の算出手段と、前記第１の出力手段より出力される乱数系列に基づいて通信文を暗号化する暗号化手段とを送信装置に具え、データを保持する第２の保持手段と、該第２の保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換する第２の変換手段と、該第２の変換手段による変換結果に基づき、前記第２の保持手段に保持されるデータを更新する第２の更新手段と、前記第２の保持手段に保持されるデータの一部を、

乱数系列として順次出力する第２の出力手段と、前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する第２の算出手段と、前記第２の出力手段より出力される乱数系列に基づいて暗号文を復号する復号手段とを受信装置に具える。

【００２３】

【作用】かかる本発明の乱数発生器においては、保持手段に保持されたデータを入力し、所定のパラメータに基づいて入力データ値を変換手段により変換し、該変換手段による変換結果に基づき、前記保持手段に保持されるデータを更新手段が更新する。出力手段が前記保持手段に保持されるデータの一部を、乱数系列として順次出力する。

【００２４】また、算出手段が前記パラメータとして出力系列から該系列を推定することが困難なパラメータ系列を順次算出してパラメータを変更する。

【００２５】また、送信側で、データを保持する第１の保持部に保持されたデータを第１の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第１の保持部に保持されるデータを更新し、前記第１の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて通信文を暗号化して暗号文を順次受信側に送信し、受信側で、データを保持する第２の保持部に保持されたデータを第２の変換部に入力し、所定のパラメータに基づいて入力データを変換し、該変換の結果に基づき、前記第２の保持部に保持されるデータを更新し、前記第２の保持部に保持されるデータの一部を、乱数系列として順次出力し、該出力される乱数系列に基づいて暗号文を復号する。

【００２６】

【実施例】

（実施例１）図１は、ＬＦＳＲを用いた乱数発生器のブロック構成を示す図である。シフトレジスタ１１及びシフトレジスタ１１の各レジスタからの値を線形変換しシフトレジスタ１１にフィードバックする線形変換回路１２からなる。

【００２７】本実施例による乱数発生の手順は以下の通りに行う（ただし手順３．４．５は同時に行われる）。

【００２８】１．シフトレジスタ１１の各レジスタに初期値を設定する。

【００２９】２．線形変換回路１２は外部から与えられるパラメータに従って線形変換を決定する。

【００３０】３．各レジスタは与えられた値を右にシフトする。

【００３１】４．最右端のレジスタの値を乱数として出力する。

【００３２】５．各レジスタの値を２．で決定された線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【００３３】６．以下３．４．５．を繰り返すが、式（２）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数（今の場合シフトレジスタの段階の２倍）より大きくなる前に線形変換回路１２に入力するパラメータを変更し、線形変換方式を変更する。

【００３４】この手順において、手順４．で出力される値の全て又は一部、或いは線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。線形変換回路にＡＮＤ回路を利用した場合の乱数発生器を図２に示す。図２において、まずシフトレジスタに初期値を設定する。ＡＮＤ回路に接続されたレジスタの値は、前述のタップ列の値h_n、h_{n-1}、…、h_2、h_1を意味するので、レジスタの値を変更すれば線形変換方式を変更することになる。出力乱数系列の数がシフトレジスタの段数の２倍を越える前にパラメータの変更によってレジスタの値を変更すれば式（２）を解くことができず、乱数列を解析することができない。

【００３５】また、手順６．において、出力される乱数の数がその乱数列により決定される線形複雑度の２倍より大きくなった後に線形変換回路に入力するパラメータを変更し、線形変換方式を変更した場合でも、式（２）により解析されるのはその線形変換方式の場合だけであり、従来例のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、パラメータによって線形変換方式を変更した後は安全である。

【００３６】（実施例２）ＬＦＳＲによる乱数発生器では、出力乱数系列の解析に必要な乱数の数はＬＦＳＲの段数の２倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数をＬＦＳＲの場合以上に大きくすることが可能である。よって、式（２）による出力乱数列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるパラメータの変更周期を大きくすることができるという利点がある。その非線形フィードバックシフトレジスタを用いた実施例を図３に示す。

【００３７】図３は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数列発生器を示すブロック図である。シフトレジスタ１１及びシフトレジスタ１１の各レジスタからの値を非線形変換しシフトレジスタ１１にフィードバックする非線形変換回路３１からなる。

【００３８】本実施例による乱数発生の手順は以下の通りに行う（ただし手順３．４．５．は同時に行われる）。

【００３９】１．シフトレジスタ１１の各レジスタに初期値を設定する。

【００４０】２．非線形変換回路３１は外部から与えられるパラメータに従って非線形変換を決定する。

【００４１】３．各レジスタは与えられた値を右にシフトする。

【００４２】４．最右端のレジスタの値を乱数として出力する。

【００４３】５．各レジスタの値を２．で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【００４４】６．以下３．４．５．を繰り返すが、式（２）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなる前に非線形変換回路に入力するパラメータを変更し、非線形変換方式を変更する。

【００４５】この手順において、手順４．で出力される値の全て又は一部、或いは非線形変換回路３１の出力の全て又は一部が本実施例によって発生される乱数となる。具体的な非線形変換回路３１の構成としては、公知の非線形関数の入出力の対応を記憶されたＲＯＭ等によって実現できる。

【００４６】（実施例３）実施例１．２．では、本発明をわかりやすく説明するため線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、上記実施例の本質は与えられた初期値をもとに、定められた変換を施してフィードバックすることにより連鎖的に乱数を発生させる乱数発生方式において、該変換における変換方式を外部より与えるパラメータによって制御すること、特に変換方式を決定するのに必要なだけの乱数列を出力する前に該変換方式を制御するパラメータを変更し、該変換方式を変更すること、にある。このことから明らかなように、乱数発生方式として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用いることができるのは言うまでもない。

【００４７】また、フィードバック変換における変換方式に関しても、外部から与えるパラメータによって制御する場合について述べてきたが、外部から与えるパラメータと内部で生成したパラメータを合成したパラメータによって制御することもできる。

【００４８】（実施例４）図４は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【００４９】本実施例では、それぞれ同一のクロックで動作するR_1～R_nのｎ個のレジスタ、各レジスタからの出力と最終レジスタ（R_n）からのフィードバック出力とで（非）線形変換を行い次のレジスタに出力するS_1～S_nのｍ個の（非）線形変換回路からなる。

【００５０】本実施例による乱数発生の手順は以下の通りに行う（ただし手順３．４．５．は同時に行われる）。

【００５１】１．各レジスタにそれぞれ初期値を設定する。

【００５２】２．S_1～S_nの各（非）線形変換回路は外部から与えられるパラメータに従って（非）線形変換を決定する。

【００５３】３．最右端のレジスタ（R_n）の値を乱数として出力し、最左端のレジスタ（R_1）の値とする。

【００５４】４．各レジスタは３．において保持していた値を出力すると同時に入力部にある値を保持する。

【００５５】５．各（非）線形変換回路は手前のレジスタから出力された値とR_nからのフィードバック出力とを２．で決定された（非）線形変換によって変換し、後のレジスタに出力する。

【００５６】６．以下３．４．５．を繰り返すが、式（２）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなる前に（非）線形変換回路に入力するパラメータを変更し、（非）線形変換方式を変更する。

【００５７】この手順において、R_nの出力の全て又は一部が本実施例によって発生される乱数となる。

【００５８】また、上記手順において、各（非）線形変換回路は前述のＲＯＭ等によって構成することができ、各（非）線形変換回路はそれぞれ異なる（非）線形変換を行っても良い。

【００５９】（実施例５）図５は擬似乱数発生器にＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号回路を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、ＤＥＳ暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。ＤＥＳ暗号回路を用いる場合は、ＤＥＳ暗号の鍵を変えることが変換方式を変えることになる。

【００６０】（実施例６）以下の実施例によれば、前述の方式Ａを用いた乱数発生器へ与えるパラメータを算出するために方式Ｂを用いたパラメータ算出回路を有し、このパラメータ算出回路より出力されるパラメータによって乱数発生器における変換方式を制御することによって、方式Ａの利点である高速性と方式Ｂの利点である安全性の２つを実現する乱数列の発生を以下のようにして可能にしたものである。

【００６１】方式Ａによる乱数発生器に出力される乱数の数が、その乱数列の解析に必要な乱数の数より大きくなる前、或いは等しくなる近辺で前記タップ列の値を変更して乱数発生手段の変換の方式を変更させることにより、式（２）の方法による出力乱数列の解析が行えないようにし、出力乱数系列の安全性を高めることができる。よって、そのタップ列の値をパラメータとして方式Ｂによって制御する。

【００６２】この場合、方式Ａを用いた乱数発生器によって出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなるまでに、方式Ｂによるパラメータの算出が行われれば良いため、方式Ｂの計算が高速に行えなくても全体として高速に乱数を生成することは可能

である。

【００６３】また、式（２）の方法で解析を行うのに十分な数の乱数を出力した後に前記のタップ列の値を変更したとしても、解析できるのはそのタップ列の値の時だけである。しかもタップ列の値の制御は方式Ｂによって行われているので次のタップ列の値を予測することは困難であり、従来のようにそれ以降の全ての乱数系列が解析されるのを防ぐことができるため、タップ列の値を変更した後は安全である。

【００６４】（実施例７）ＬＦＳＲによる乱数発生器では、出力乱数系列の解析に必要な乱数の数はＬＦＳＲの段数の２倍であるが、非線形フィードバックシフトレジスタを用いた場合には解析に必要な乱数の数をＬＦＳＲの場合以上に大きくすることが可能である。よって、式（２）による出力乱数列の解析に必要なビット数が多くなるので、非線形変換の方式を変えるためのパラメータの算出周期を大きくすることができるという利点がある。算出周期を大きくできることは、高速処理の困難な方式Ｂをパラメータ算出部に用いる場合に特に大きな利点となる。

【００６５】その非線形フィードバックシフトレジスタを用いた実施例を図８に示す。図８は本発明による非線形フィードバックシフトレジスタを用いた場合の乱数列発生器を示すブロック図である。方式Ａに基づく乱数発生手段としてシフトレジスタ及びシフトレジスタの各レジスタからの値を非線形変換しシフトレジスタにフィードバックする非線形変換回路２１を用い、方式Ｂに基づくパラメータ算出回路６１を用いて構成される。非線形変換方式はパラメータ算出回路６１からの出力により制御される。

【００６６】本実施例による乱数発生手順は以下の通りに行う（ただし手順４．５．６．は同時に行われる）。

【００６７】１．シフトレジスタの各レジスタ及びパラメータ算出回路に初期値を設定する。

【００６８】２．パラメータ算出回路は与えられた初期値から第一のパラメータを算出し、非線形変換回路２１に出力する。

【００６９】３．非線形変換回路２１は、２．により与えられるパラメータに従って非線形変換を決定する。

【００７０】４．各レジスタは与えられた値を右にシフトする。

【００７１】５．最右端のレジスタの値を乱数として出力する。

【００７２】６．各レジスタの値を３．で決定された非線形変換に従ってフィードバック変換し、最左端のレジスタの値とする。

【００７３】７．以下４．５．６．を繰り返すが、式（２）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパラメータを算出し、非線形変換回路２１に出力して非線形変換方式を変更する。

【００７４】この手順において、手順５．で出力される値の全て又は一部、或いは非線形変換回路の出力の全て又は一部が本発明によって発生される乱数となる。具体的な非線形変換回路２１の構成としては、公知の非線形関数の入出力の対応を記憶させたＲＯＭ等によって実現できる。

【００７５】（実施例８）実施例６、７では、本発明をわかりやすく説明するため乱数発生手段として線形及び非線形フィードバックシフトレジスタを用いた例について述べたが、本発明の本質は方式Ａを用いた乱数発生手段の変換方式を方式Ｂを用いたパラメータ算出手段から出力されるパラメータによって制御することにある。特に乱数発生手段の変換方式を決定するのに必要なだけの乱数列を出力する前に該変換方式をパラメータ算出手段からの出力により変更することにある。このことから明らかなように、乱数発生手段として線形及び非線形フィードバックシフトレジスタに限らず、種々の方式を用いることができるのは言うまでもない。

【００７６】また、方式Ｂとして用いることのできる暗号学的に安全な擬似乱数発生法には、式（３）の他に文献「暗号と情報セキュリティ」（辻井、笠原著、１９９０年発行、株式会社昭晃社、８６頁）に示されているように、ＲＳＡ暗号、離散対数、逆数暗号を用いたものが知られており、これらも本発明のパラメータ算出手段のアルゴリズムに用いることができる。

【００７７】また、図２のように暗号学的に安全な擬似乱数発生法と内容が秘密にされたＲＯＭをフィードバック的に用いる方法を組み合わせることによっても方式Ｂに基づくパラメータ発生手段は構成できる。

【００７８】また、内容が秘密にされたＲＯＭをフィードバック的に用いる方法だけによっても、それまでにそのＲＯＭから発生した値からＲＯＭ内部の残りの値を知ることはできないため、方式Ｂに基づくパラメータ発生手段は構成できる。

【００７９】さらに、乱数発生手段の変換方式の制御に関してもパラメータ算出回路により生成されたパラメータによってのみ制御する場合について述べてきたが、乱数発生手段の内部のパラメータとパラメータ算出回路で算出したパラメータとを合成したパラメータによって制御することもできる。

【００８０】（実施例９）図９は、乱数を発生させる手順としてシフトレジスタを用いない場合を示している。

【００８１】本実施例では、方式Ａに基づく乱数発生手段としてそれぞれ同一のクロックで動作するR_1～R_sのｓ個のレジスタ及び各レジスタからの出力と最終レジスタ（R_s）からのフィードバック出力とで（非）線形変換を行い次のレジスタに出力するT_1～T_sのｍ個の（非）線形変換回路を用い、方式Ｂに基づくパラメータ

算出回路６１を用いて構成される。各（非）線形変換方式はパラメータ算出回路６１からの出力により制御される。

【００８２】本実施例による乱数発生の手順は以下の通りに行う（ただし手順４．５．６．は同時に行われる）。

【００８３】１．各レジスタ及びパラメータ算出回路６１ににそれぞれ初期値を設定する。

【００８４】２．パラメータ算出回路６１は与えられた初期値から第一のパラメータを算出し、各（非）線形変換回路に出力する。

【００８５】３．T_1 ～T_n の各（非）線形変換回路は２．により与えられるパラメータに従ってそれぞれの（非）線形変換を決定する。

【００８６】４．最右端のレジスタ（R_n）の値を乱数として出力し、最左端のレジスタ（R_1）の値とする。

【００８７】５．各レジスタは４．において保持していた値を出力すると同時に入力部にある値を保持する。

【００８８】６．各（非）線形変換回路は手前のレジスタから出力された値とR_nからのフィードバック出力とを３．で決定された（非）線形変換によって変換し、後のレジスタに出力する。

【００８９】７．以下４．５．６．を繰り返すが、式（２）による出力乱数列の解析が行えないようにするため、出力される乱数の数がその乱数列の解析に必要な乱数の数より大きくなる前にパラメータ算出回路は次のパラメータを算出し、各（非）線形変換回路に出力してそれぞれの（非）線形変換方式を変更する。

【００９０】この手順において、R_nの出力の全て又は一部が本発明によって発生される乱数となる。

【００９１】また、上記手順において、各（非）線形変換回路は前述のＲＯＭ等によって構成することができ、各（非）線形変換回路はそれぞれ異なる（非）線形変換を行っても良い。

【００９２】（実施例１０）図１０は本発明において乱数発生手段にＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号回路５１を用いる場合の実施例を示している。最近差分解読法と呼ばれる有力な解読法が提案され、ＤＥＳ暗号の安全性に疑問が持たれるようになっており、その対策として鍵を頻繁に変更することが考えられる。ＤＥＳ暗号装置５１を用いる場合は、ＤＥＳ暗号の鍵を変えることが変換方式を変えることになる。

【００９３】（実施例１１）これまでに述べたように、上記の乱数発生器によって生成された乱数は解析に対して強いので、この乱数を暗号化方式に用いることにより解析に対して強く安全性の高い暗号通信が実現できる。以下、通信文と乱数との間でビット毎に排他的論理和をとる暗号化方式（ストリーム暗号）による暗号通信ネットワークにおいて、乱数発生器を用いた暗号通信の実施例を示す。

【００９４】図１１はネットワークの加入者間で固有かつ秘密の暗号鍵を共有している共通鍵暗号通信ネットワークを示し、Ａ、Ｂ、Ｃ、…、Ｎはそのネットワークの加入者、K_{AB}、K_{AC}、…はそれぞれ加入者Ａ－Ｂ間で共有している暗号鍵、加入者Ａ－Ｃ間で共有している暗号鍵、…を示している。

【００９５】図１２は本発明による乱数発生回路とパラメータ算出回路からなる乱数発生器１２１を用いた場合の暗号装置及び復号装置を含む通信装置１２２の構成を示したブロック図である。

【００９６】図１３は図１１、図１２で示された暗号通信システムにおけるＡ、Ｂ間の秘匿通信の様子を示している。

【００９７】加入者Ａから加入者Ｂへの暗号通信は以下の手順で行う。

【００９８】１．通信の送信者Ａは、送信先Ｂと共有している秘密の鍵K_{AB}の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、乱数系列k_iを発生させる。

【００９９】２．Ａは発生した乱数系列k_iと通信文m_iをビット毎に排他的論理和をとり、暗号文

【０１００】

【外３】

$$c_i = m_i \oplus k_i$$

を計算し、その暗号文をＢに送信する。

【０１０１】３．通信の受信者Ｂは、送信元Ａと共有している秘密の鍵K_{AB}の全て又は一部を乱数発生回路及びパラメータ算出回路の初期値として設定し、送信者が発生したのと同じ乱数系列k_iを発生させる。

【０１０２】４．Ｂは発生した乱数系列k_iと受信暗号文c_iをビット毎に排他的論理和をとり、通信文

【０１０３】

【外４】

$$m_i = c_i \oplus k_i$$

を復元する。

【０１０４】この手順に従えば、正規の送信先Ｂだけがその秘密の鍵K_{AB}を知っているので受け取った暗号文を本来の通信文に復号でき、それ以外の加入者（Ｃ～Ｎ）はその暗号文をする際に用いられた秘密の鍵を知らないのでその内容を知ることができない。このことにより秘匿通信が実現される。また、図１１のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいても、公知の手法で鍵共有を行えば同じ手順で暗号通信を実現することができる。

【０１０５】（実施例１２）実施例１１に示した暗号通信ネットワークでは通信文の送信者と受信者の間で固有

15

かつ秘密の鍵を共有しているので、暗号文を受け取り、意味をなす通信文に復号できるということは、通信文がその鍵のもう一人の所有者から送信されたことを受信者に保証している。そのため、実施例１１に示した秘匿通信システムでは、通信の発信者及び着信者の認証も行うことができる。

【０１０６】（実施例１３）実施例１１、１２のようにあらかじめ暗号鍵が配布されているのではなく、暗号通信を行うに先立って送・受信者間で暗号鍵を共有する必要がある形態のネットワークにおいて、盗聴の可能性のある通信路を介した場合でも安全に暗号鍵を共有できる方式としてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎの方式（W. Diffieand M. E. Hellman “New Directions incryptography”, IEEE, IT, vol. I. T－22, No. 6, １９７６）がよく知られている。その際に用いる乱数として本発明により発生した乱数を用いることができる。

【０１０７】その場合に用いる乱数は、送信者と着信者で同じものを持つ必要はないため、乱数発生手段及びパラメータ発生手段に設定する初期値は任意の値を用いれば良い。

【０１０８】

【発明の効果】以上説明したように、本発明によれば、一定数の出力系列から解析可能な方式（方式Ａ）により出力される乱数の数が、その解析に必要な数より大きくなる前、或いは等しくなる近辺で、方式Ａのパラメータを変更するので、方式Ａの解析に必要な数の出力を集めることが困難になり、発生する乱数の安全性が高められるという効果がある。

【０１０９】また、方式Ａのパラメータを、出力系列から解析困難な方式（方式Ｂ）により出力される乱数に基づいて変更することにより、方式Ａの安全性が一層高められるという効果がある。

【０１１０】この場合、方式Ａから出力される出力の数が方式Ａの解析に必要な数より大きくなるまでに、方式Ｂによる乱数の出力が行われれば良いため、方式Ｂの乱数発生は高速に行えなくてもよい。しかし、最終出力は方式Ａからの出力であるので、高速に乱数を発生することが可能である。

【０１１１】また、この乱数系列を暗号通信に用いれば、高速かつ安全性の高い暗号通信が実現されるという

16

効果がある。

【図面の簡単な説明】

【図１】ＬＦＳＲを用いた乱数発生器のブロック構成を示す図である。

【図２】ＬＦＳＲを用いた乱数発生器の詳細なブロック構成を示す図である。

【図３】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図４】複数個のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図５】ＤＥＳ暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図６】ＬＦＳＲを用いた乱数発生器のブロック構成を示す図である。

【図７】ＬＦＳＲを用いた乱数発生器のブロック構成を示す図である。

【図８】非線形フィードバックレジスタを用いた乱数発生器のブロック構成を示す図である。

【図９】複数個のレジスタを用いた乱数発生器のブロック構成を示す図である。

【図１０】ＤＥＳ暗号装置を用いた乱数発生器のブロック構成を示す図である。

【図１１】共通鍵暗号通信ネットワークを説明する図である。

【図１２】暗号装置及び復号装置を含む通信装置の構成を示すブロック図である。

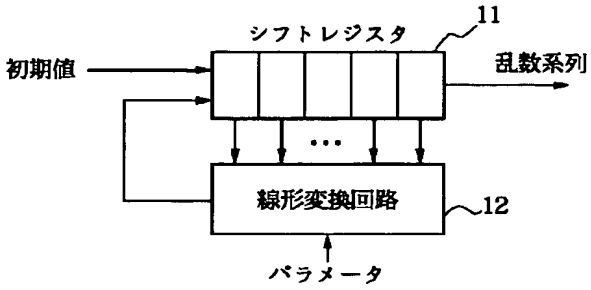
【図１３】秘匿通信を行う通信システムを説明する図である。

【図１４】ＬＦＳＲを用いた従来の乱数発生器のブロック構成を示す図である。

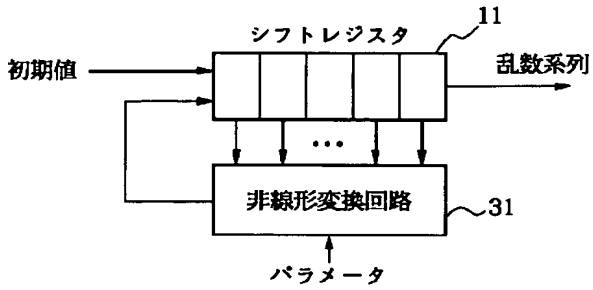
【符号の説明】

１１　シフトレジスタ
１２　線形変換回路
２１　レジスタ
３１　非線形変換回路
５１　ＤＥＳ暗号回路
６１　パラメータ算出回路
７１　ＲＯＭ
７２　バッファ
７３　自乗剰余算回路
１２１　乱数発生器
１２２　通信装置

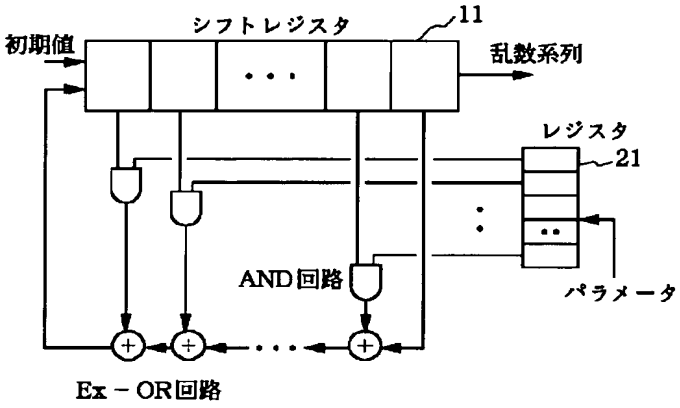
【図１】



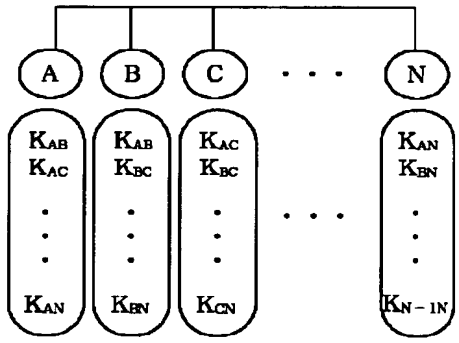
【図３】



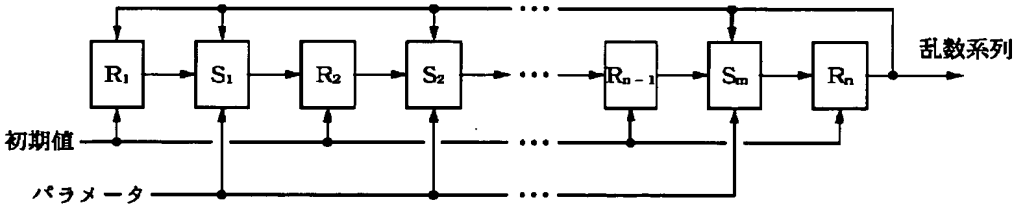
【図２】



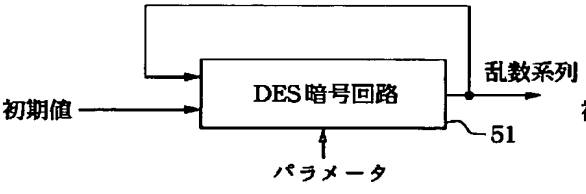
【図１１】



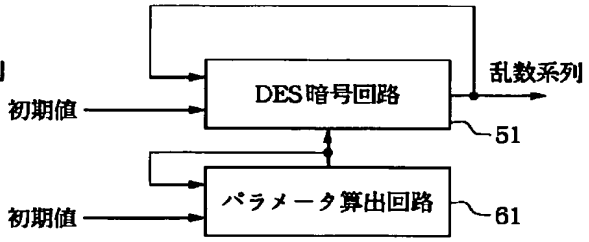
【図４】



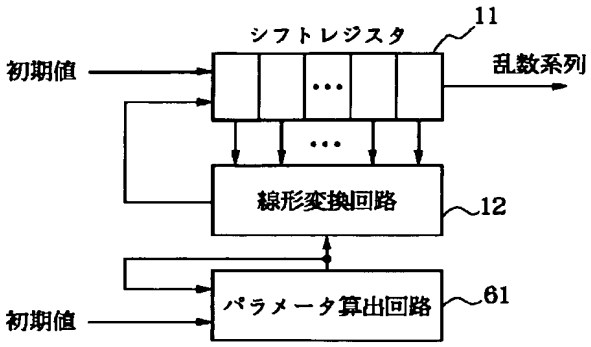
【図５】



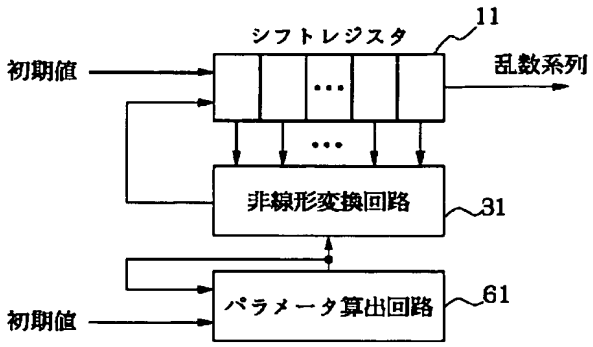
【図１０】



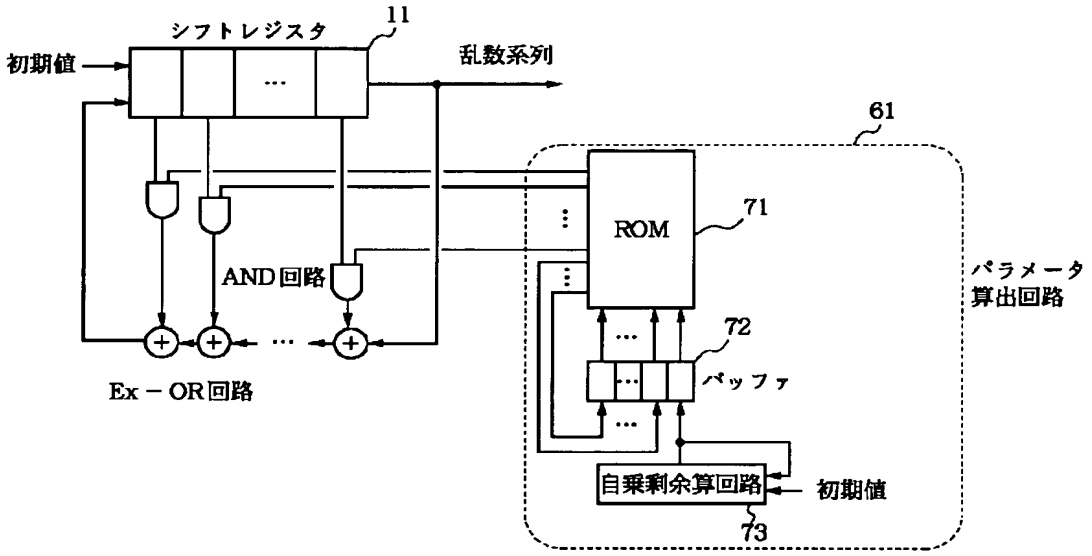
【図６】


シフトレジスタ
11
初期値
乱数系列
線形変換回路
12
初期値
パラメータ算出回路
61

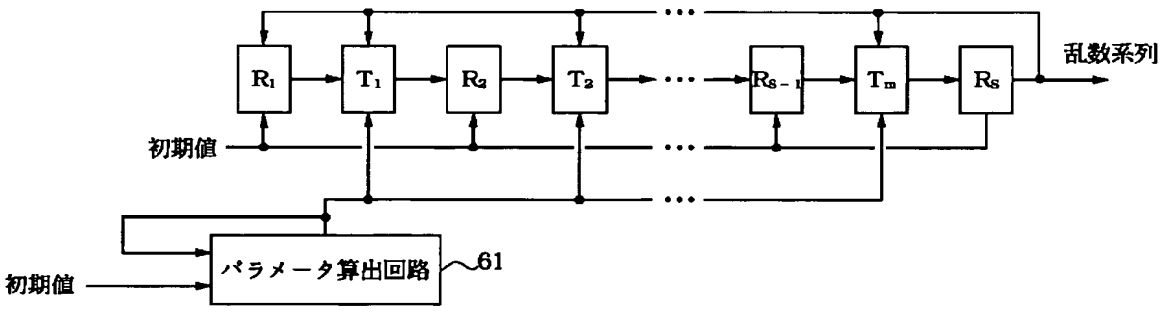
【図８】


シフトレジスタ
11
初期値
乱数系列
非線形変換回路
31
初期値
パラメータ算出回路
61

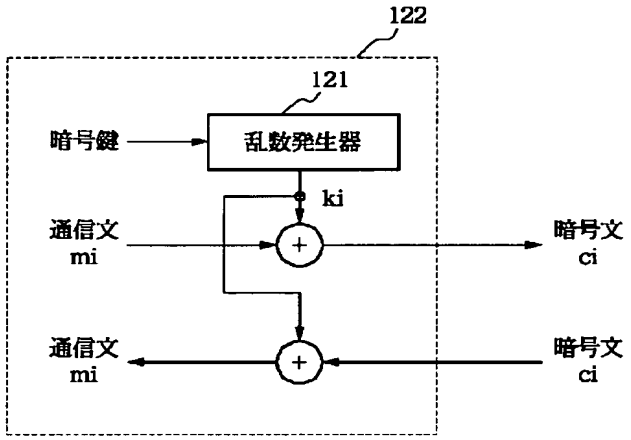
【図７】


シフトレジスタ
11
初期値
乱数系列
61
ROM
71
AND回路
パラメータ
算出回路
72
バッファ
Ex－OR回路
自乗剰余算回路
初期値
73

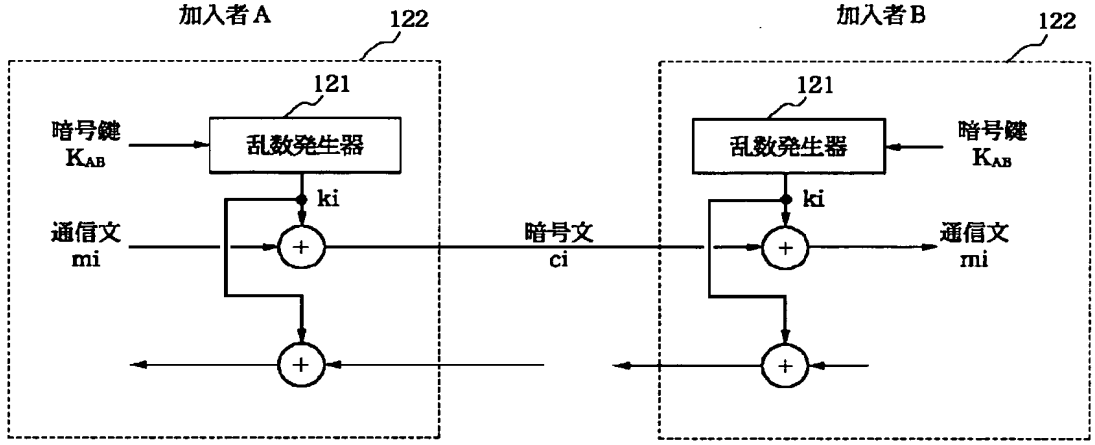
【図９】


R1
T1
R2
T2
Rs－1
Tm
Rs
乱数系列
初期値
初期値
パラメータ算出回路
61

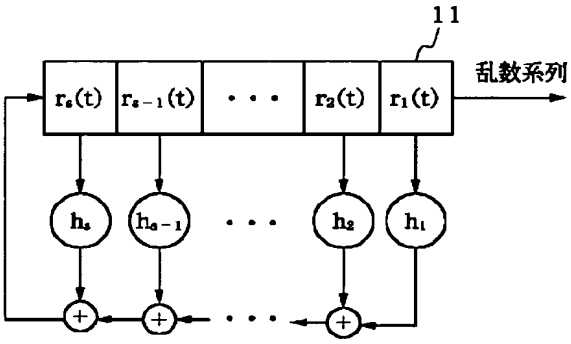
【図１２】


122
121
暗号鍵
乱数発生器
ki
通信文
mi
暗号文
ci
通信文
mi
暗号文
ci

【図１３】


加入者Ａ
122
121
暗号鍵
K_{AB}
乱数発生器
ki
通信文
mi
暗号文
ci
加入者Ｂ
122
121
乱数発生器
暗号鍵
K_{AB}
ki
通信文
mi

【図１４】


11
$r_s(t)$
$r_{s-1}(t)$
・・・
$r_2(t)$
$r_1(t)$
乱数系列
h_s
h_{s-1}
・・・
h_2
h_1